TSA Registered Traveler

Security, Privacy and Compliance Standards for Sponsoring Entities and Service Providers

Version 3.0, May 2007

Transportation Security Administration

RT Registered Traveler™

Table of Contents

List of Figures and Tables

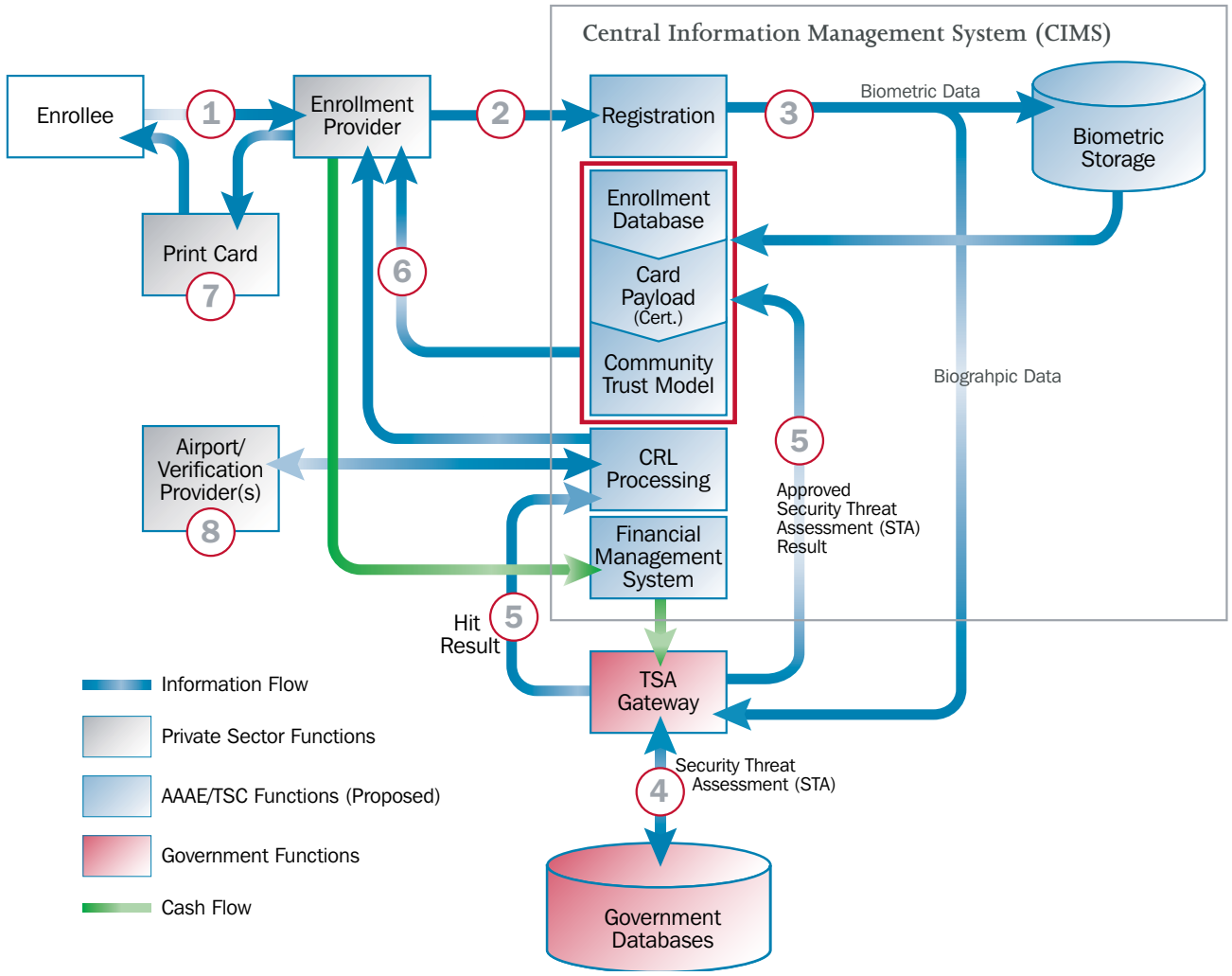
1. Introduction

The Registered Traveler (RT) concept, as indicated in the RT model, has been authorized under the Aviation and Transportation Security Act (ATSA) as a means to "**establish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such programs.**" To establish an interoperable, vendor-neutral RT Program for airline travel, the Transportation Security Administration (TSA) will partner with the private sector using a public-private partnership model. Sponsoring Entities (SEs) and Service Providers (SPs) will provide the necessary systems, processes and support for the RT Program. SEs will contract with SPs through the SEs' own acquisition processes.

Each SE will conduct oversight of its SP, which also will be subject to oversight by TSA in accordance with the standards set forth in this document. TSA will retain responsibility for those functions that are inherently governmental, including: (1) establishing standards for the operation of the RT Program by SEs and SPs, (2) monitoring compliance with those standards on an ongoing basis, (3) conducting TSA security threat assessments and adjudications, and (4) performing physical screening at TSA security checkpoints.

As described in the RT model, TSA requires that SPs demonstrate interoperability with the Central Information Management System (CIMS). The overarching RT enterprise architecture depicted in figure 1-1 highlights high-level interconnections among the SPs, the CIMS, and TSA. An Enrollment Provider (EP) collects biographic and biometric information from an RT applicant and transmits the data to the CIMS. The CIMS formats and transmits the data to TSA. TSA conducts an initial security threat assessment, re-vets on a perpetual basis, and transmits an "approved" or "not-approved" finding back to the CIMS. The CIMS informs the EP of acceptance or nonacceptance, and the EP then informs the RT applicant and issues a card if he or she is approved. When an RT Participant travels through a participating airport, he or she uses the RT card at an RT verification station, which confirms the individual's identity and current status in the program.

Figure 1-1. RT Information Flow



TSA established the RT Security, Privacy and Compliance Standards for Sponsoring Entities and Service Providers (known as the RT Standards) by garnering leading practices from the private sector and from government. During phase 1 of this process, TSA:

- Researched applicable existing guidance and government regulations pertaining to information security, privacy, public-private partnerships, foreign-owned or foreign-controlled entities as government contractors and auditing standards;
- Conducted a vulnerability assessment of RT processes to identify and prioritize key risks to the program, ensuring that program standards address areas of high risk;
- Considered standards from other public-private partnership programs within government, as well as private sector partnership programs; and
- Applied a standards-based approach for ensuring and maintaining an end-to-end chain of trust for personal privacy information.

In phase 2, TSA carefully considered feedback from interested stakeholders and incorporated applicable updates into the final version of this standard.

1.1 Purpose

This document gives prospective SEs and SPs a comprehensive description of TSA's security, privacy, and compliance standards for the information systems supporting RT.

This document contains the following sections:

- **Information Systems Security Standards:** guidelines for securing SP information systems and the data that RT Participants have entrusted to them.
- **Enrollment/Verification Standards:** process-specific guidelines for establishing internal control over enrollment and verification processes.
- **Ongoing Compliance:** procedures for monitoring SP compliance with the standards.

1.2 Definitions

Table 1-1 Glossary of Terms

Term	Definition
Aircraft Operator Standard Security Program (AOSSP)	A standardized program for domestic aircraft operators of flights, both in the United States and overseas, that are regulated in accordance with 49 C.F.R. Part 1544. The program contains requirements for areas such as training, screening and aircraft security.
Airport Security Program (ASP)	An airport's local security program. National amendments to ASPs are issued from TSA headquarters requiring amendments to all local programs. There is no standardized program for airport operators regulated in accordance with 49 C.F.R. Part 1542.
Availability	The extent to which access to and use of information is timely and reliable. A loss of availability is the disruption of access to or use of information or an information system.
Biometrics	Measurable, physiological characteristics that are unique to an individual, such as a fingerprint or iris scan.

Term	Definition
Central Information Management System (CIMS)	A system to aggregate, store and distribute information (on an as-needed basis) to the entities participating in the RT Program. Responsibilities include: receiving, aggregating and formatting RT applicant data from EPs; performing checks that identify potential duplicate enrollments to ensure application integrity; transmitting applicant data to TSA for the agency to conduct security threat assessments (e.g., checks against government databases to determine eligibility for RT status); receiving determinations of eligibility from TSA; maintaining and distributing the Card Revocation List (consisting of unique identifiers); and generating the biometric payload and cryptographic protocols for RT cards.
Compliance	Conformity with the standards and requirements set forth in the *TSA Registered Traveler Security, Privacy and Compliance Standards for Sponsoring Entities and Service Providers*.
Confidentiality	Preservation of authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
Enrollment	The process of submitting an application to participate in the RT Program by providing biographic and biometric information for a TSA security threat assessment.
Enrollment Provider (EP)	An RT SP that collects the biographical and biometric information from RT applicants, collects user fees from RT applicants and issues RT cards to RT Participants. An EP may be the same entity as a Verification Provider (VP).
Graphical User Interface (GUI)	A user interface based on graphics (icons, pictures and menus) instead of or in addition to text.
Independent Verification and Validation (IV&V)	The process by which a qualified, unrelated and unbiased entity checks that a system is properly and effectively designed (verification) and that it performs as intended (validation).
Integrity	Protection against improper information modification or destruction; includes ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
Interconnection Security Agreement (ISA)	A document that specifies the technical and security requirements for establishing, operating and maintaining interconnection. It also supports the memorandum of understanding/agreement (MOU/MOA) between the organizations. Specifically, the ISA documents the requirements for connecting the information technology (IT) systems, describes the security controls that will be used to protect the systems and data, contains a topological drawing of the interconnection and provides a signature line.
Interoperability	The technical capability for any RT credential legitimately issued by an EP to work at the verification station of any authorized VP.

Term	Definition
Model Security Plan (MSP)	The foreign air operator security plan that must be applied in order for foreign airlines to operate in and out of U.S. airport locations.
National Institute of Standards and Technology (NIST)	A nonregulatory federal agency within the U.S. Department of Commerce's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve quality of life.
Personally Identifiable Information/Personally Identifying Information (PII)	Any item, collection or grouping of information about any person that contains: a person's name; a unique identifying number, such as a Social Security, passport or driver's license number; or other identifying particular assigned to that person, such as a symbol, fingerprint or photograph. Source: Office of Transportation Security Policy, TSA Management Directive No. 2100.2, Privacy and Information Collection Policy.
Privacy Act	A federal statute that forbids the disclosure of specific material held by federal agencies on the grounds that its release could invade the privacy of the subject of the report or document. 5 United States Code (U.S.C.) Section 552a.
Registered Traveler Interoperability Consortium (RTIC)	A consortium formed to establish common RT business rules and technical standards necessary for an open, secure and industry-driven network that will create a fair and seamless platform for airports, airlines and vendors to interface with TSA and each other.
RT Applicant	An individual who has supplied biographical and biometric data voluntarily to an RT EP with the intent of joining RT and paying the associated user fee.
RTIC Technical Interoperability Specification Version 1.0	A specification document developed by the RTIC to help foster a fully interoperable, vendor-neutral RT Program within the United States.
RT Line	A queue (either designated or dedicated) to the TSA screening operation for the use of RT Participants that leads to the TSA security checkpoint.
RT Participant	An individual who has enrolled voluntarily with an EP, receives and maintains an approved security threat assessment from TSA and meets all other requirements set by TSA.
Security Checkpoint	A section of the airport that all passengers must traverse to reach the gate area. The location at which passengers and carry-on baggage are screened by TSA for potential threats and hazards.
Security Threat Assessment	The process by which TSA determines an RT applicant's initial eligibility for the program, as well as an RT Participant's continued eligibility. The security threat assessment includes checks against federal government databases to determine whether the individual poses or is suspected of posing a threat to transportation or national security.

Term	Definition
Service Provider (SP)	A term of collective reference for VPs and EPs.
Sponsoring Entity (SE)	An airport or air carrier, subject to TSA regulations, that manages the RT Program at a particular site or sites. These entities select and qualify all participating SPs in accordance with TSA RT Standards.
System Security Plan (SSP)	Documents the approach to implementing operational, technical and management security controls across a system and delineates responsibilities and expected behavior of all individuals who access the system.
Verification Provider (VP)	An SP that verifies the identity of the RT Participant at the airport. The VP may be the same entity as an EP.

2. Information Systems Security Standards

The RT information systems security standards are designed to ensure that SEs and SPs deploy secure information systems and processes, which then protect the confidentiality, integrity and availability of entrusted RT Participant data. TSA's intent is for RT information systems security standards to promote consistent and repeatable security controls in SP information systems without placing undue burden on SEs and SPs.

RT information systems security standards will:

- Provide a complete, risk-based and cost-effective security approach to achieve approval to provide RT services;
- Leverage standardized templates and reporting formats for security requirement traceability from a program and validation and verification perspective; and
- Emphasize management, operational and technical security controls that do not hinder interoperability requirements.

TSA has established a minimum set of baseline information systems security standards, using NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, for securing RT information systems as outlined in Appendix C. The objective of NIST Special Publication 800-53 is to provide security controls that are consistent with and complementary to other established security standards. The catalog of security controls provided in NIST Special Publication 800-53 can be used effectively to demonstrate compliance with a variety of governmental, organizational or institutional security standards. NIST Special Publication 800-53 is a widely recognized body of security criteria for federal systems and currently is being adopted by private sector and industry partners as the de facto standard.

RT information systems security standards are organized into three classes listed in table 2-1, Security Control Families: management, operational and technical. Management controls focus on security systems program risk. Operational controls address security methods or mechanisms that are implemented by people (as opposed to systems). Technical controls manage the security controls executed by the RT systems. These controls provide automated protection from unauthorized access or misuse, facilitate detection of security violations and support security requirements for applications and data.

Table 2-1. Security Control Families

Class	Family	Identifier
Management	Risk Assessment	RA
	Planning	PL
	System and Services Acquisition	SA
Operational	Personnel Security	PS
	Physical and Environmental Protection	PE
	Contingency Planning	CP
	Configuration Management	CM
	Maintenance	MA
	System and Information Integrity	SI
	Media Protection	MP
	Incident Response	IR
	Awareness and Training	AT
Technical	Identification and Authentication	IA
	Access Control	AC
	Audit and Accountability	AU
	System and Communications Protection	SC

2.1 Federal Information Processing Standards (FIPS) 199 Security Categorization

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, establishes security categories for both federal information and information systems. The security categories are based on the potential impact should certain events occur. Specifically, the controls pertain to events that jeopardize the information and information systems needed to accomplish the RT assigned mission, protect its assets, maintain its day-to-day functions and protect RT Participant data. NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, is a companion guide to FIPS Publication 199 and provides suggested standard information "types" for all federal systems.

TSA established initial security categorizations for RT information systems using FIPS Publication 199. TSA determined that the initial security categorization for confidentiality and integrity will be **High**, and availability will be **Moderate** based on analysis of potential impact as described in table 2-2, Summary of Potential Impact Definitions. Therefore, security controls should be applied that are commensurate with a **High** security category system. NIST Special Publication 800-53 contains implementation requirements for this categorization. Any controls that cannot be met should be documented in an SSP accompanied by a mitigation plan or explanation of a compensating control.

Table 2-2. Summary of Potential Impact Definitions

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C. Sec. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets or individuals.
Integrity Guarding against improper information modification or destruction; includes ensuring information nonrepudiation and authenticity. [44 U.S.C. Sec. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C. Sec. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets or individuals.

2.1.1 Rationale

The RT SP information systems, data and business processes are unique because they are governed by a partnership between TSA, via the SE, and private industry. This categorization was derived from NIST Special Publication 800-60, *Volume II: Guide for Mapping Types of Information and Information Systems to Security Categories.*

The rationale affecting the RT information systems security categorization is summarized in table 2-3, SP Security Categorization Rationale.

Table 2-3. SP Security Categorization Rationale

NIST 800-60 Criteria	Information Types	Security Categorization Rationale
C.2.8.7	Central Records and Statistics Management Information	• Unauthorized disclosure of centrally managed records can pose a threat to human life or a loss of major assets.
C.2.8.9	Personal Identity and Authentication Information	• Large aggregate tort awards can result from large-scale disclosure of personal identity and authentication information. • Potential financial hardship and identity theft can affect citizens. • Personal identity and authentication information is used to control access to facilities (e.g., sensitive facilities, critical infrastructure facilities, key national assets) or for border control purposes. • Data modification permits access to sensitive facilities by individuals to whom access should be prohibited.
C.3.1.4	Travel Information	• Unauthorized disclosure of PII coupled with credit information (e.g., name, date of birth, credit card number) can result in serious consequences or hardship for participants.
C.3.5.6	Record Retention Information	• Unauthorized disclosure of PII coupled with credit information (e.g., name, date of birth, credit card number) can result in serious consequences for participants.
D.2.1	Border and Transportation Security Information	• Unauthorized disclosure of border control information may put the physical safety of personnel and citizens in serious jeopardy. • Unauthorized disclosure of confidential information associated with ensuring security of transportation and infrastructure networks, facilities, vehicles and personnel within the United States can result in facilitation of terrorist activities that endanger human life.
D.16.3	Citizen Protection Information	• Unauthorized modification or destruction of citizen protection information can result in loss of human life. • Threats to critical infrastructures, key national assets and human life.

2.1.2 Description of Information Systems Security Standards

Table 2-4 provides a summary of RT information systems security standards. Appendix C provides additional guidance.

Table 2-4. Summary of RT Standards

Security Control Family	Description	Summary of RT Standards
Risk Assessment	The process of identifying risks to SE and SP operations (including mission, functions, image or reputation), assets or individuals by determining the probability of occurrence, the resulting impact and additional security controls that would mitigate this impact.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, risk assessment policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. The SP must implement the policy and perform a risk assessment. TSA recommends NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, as a guideline for conducting risk assessments.
Planning	The process of formally developing and approving security policy and documenting procedures that implement security controls.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.
System and Services Acquisition	The development and implementation of formal policies and procedures governing the acquisition of systems.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
Personnel Security	Those practices, technologies and/or services used to ensure that personnel security safeguards are applied.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. In addition to the NIST standards, due to the level of access to PII, TSA requires that all SP employees with access to PII be subject to a Criminal History Record Check (CHRC) and TSA security threat assessment. TSA will provide guidance to the SPs on how to submit the necessary paperwork for a CHRC and security threat assessment.

Security Control Family	Description	Summary of RT Standards
Physical and Environmental Protection	The protection of information infrastructure from unauthorized physical access or avoidable damage.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
Contingency Planning	The planning for backup procedures, emergency response, and postdisaster recovery.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. TSA recommends NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, as a basis for contingency planning.
Configuration Management	The detailed recording and updating of information that describes an enterprise's computer systems and networks, including all hardware and software components.	The SP must have a robust configuration management program. This program will develop, implement and maintain and periodically review/update: (1) a formal, documented, configuration management policy and plan that address purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the configuration management policy and plan with associated configuration management controls.
Maintenance	The modification of a system to correct faults, to improve performance or to adapt the system to a changed environment or changed requirements.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
System and Information Integrity	The quality of system or information when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Security Control Family	Description	Summary of RT Standards
Media Protection	The protection of information system media, both paper and digital; the limitation of access to information on information system media to authorized users; and the sanitizing or destroying of information system media before disposal or release for reuse.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.
Incident Response	The practice of detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem and documenting each step of the response for future reference.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
Awareness and Training	The process of ensuring that all individuals are appropriately trained in how to fulfill their security, privacy and user responsibilities before allowing them to access or administer the system.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, security/privacy awareness and training policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. In addition, the SP provides trained and knowledgeable staff. SP staff is prepared to respond to public inquiries, including inquiries about its role in the program, enrollment operations and its privacy policy. SP staff will undergo a full criminal history background check and will not be authorized to work for the SP if they have committed any of the disqualifying criminal offenses. The SP trains staff to recognize the acceptable documents used to establish identity (see Section 3.4.4) and to be knowledgeable about the characteristics of the documents that indicate validity. The SP trains staff to use a document authentication device or other method used to meet the requirements in Section 3.4.4.
Identification and Authentication	The technical measures that prevent unauthorized people (or unauthorized processes) from entering a computer system.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Security Control Family	Description	Summary of RT Standards
Access Control	The ability to permit or deny the use of an object (a passive entity, such as a system or file) by a subject (an active entity, such as an individual or process).	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
Audit and Accountability	The examination of the controls within an entity's IT infrastructure. The process of collecting and evaluating evidence of an organization's information systems, practices and operations.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
System and Communications Protection	The measures and controls that ensure confidentiality, integrity and availability of the information processed and stored by automated information systems.	The SP develops, disseminates and periodically reviews/updates: (1) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities and compliance; and (2) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

2.2 System Security Plan

SPs shall create SSPs to document their approach to implementing management, operational and technical security controls across the RT system based on guidance from NIST Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*.

All information systems operated by an SP, or a third party in support of an SP, that either directly or indirectly support a RT Program shall be included within the scope of the security, privacy and compliance requirements. One SSP shall be prepared for each system that forms the SP's RT IT program for each supported airport. A "separate" system is one that has a distinct logical or physical boundary that separates it from other systems that are part of the SP's RT IT program. If the SP's RT IT program is implemented using a monolithic system, with one set of security controls that secure all the information needed to support the RT Program, only one SSP is needed. If the SP's RT IT program uses a collection of systems, or a distributed computing environment, a unique SSP shall be developed for each system or distributed environment. This requirement will facilitate the collection of specific, detailed security information for each unique system instead of creating language in a large, voluminous plan that documents multiple security controls across multiple systems. The requirement also will facilitate execution of the self-assessment (see Section 4.1), so the results collected will reflect the appropriate level of granularity and will not result in generalized expressions of the self-assessment results.

The SSP shall delineate responsibilities and expected behavior of all individuals who access the system. Also, it shall reflect input from various managers with responsibilities concerning the system, including information owners, the system owner and the Information Security Officer (ISO). It shall describe how the required security controls are implemented, operated and maintained within that system. It shall describe its interconnection or relationship with other systems with which it exchanges information. Additional information may be included in the basic plan, and the structure and format

may be organized according to SP needs, as long as the major sections described in this document are adequately covered and readily identifiable.

SSPs shall include, at a minimum, the information in table 2-5, Minimum Security Plan Information. The policies and procedures described in table 2-4, Summary of RT Standards, shall be included in the appropriate locations within the SSPs. Sufficient detail shall be provided to facilitate an effective assessment of the efficacy of the policies and procedures. Appendix E provides a Sample SSP Template.

Table 2-5. Minimum Security Plan Information

Item	Description
Information System Name/Title	Unique identifier and name given to the system.
Information System Security Categorization (FIPS 199)	Per Section 2.1, the initial Information System Security Categorization for RT systems is **High**.
Information System Owner	Name, title, department, address, e-mail address and phone number of person who owns the system.
Authorizing Senior Management	Name, title, department, address, e-mail address and phone number of the senior management official designated as the authorizing official.
Other Designated Contacts	List other key personnel, if applicable; include their name, title, address, e-mail address and phone number.
Assignment of Security Responsibility	Name, title, address, e-mail address and phone number of person who is responsible for the security of the system.
Information System Operational Status	Indicate the operational status of the system. If more than one status is indicated, list which part of the system is covered under each status.
Information System Type	Indicate the information system type. If the system contains minor applications, list them in the General System Description/Purpose section.
General System Description/ Purpose	Describe the function or purpose of the system and the information processes.
System Environment	Provide a general description of the technical system. Include the primary hardware, software and communications equipment.
System Interconnections/ Information Sharing	List interconnected systems and system identifiers (if appropriate); provide the system name, organization and system type (major application or general support system); indicate if there is an ISA/MOU/MOA on file; and provide the date of agreement to interconnect, FIPS 199 category and the name of the authorizing official.

Item	Description
Related Laws/ Regulations/Policies	List any laws or regulations that establish specific requirements for the confidentiality, integrity or availability of the data in the system.
Minimum Security Controls	The description shall contain: (1) the security control title, (2) how the security control is being implemented or is planned to be implemented, (3) any scoping guidance that has been applied and the type of consideration and (4) an indication that the security control is a common control and the person who is responsible for its implementation. (See Appendix C.)
Information SSP Completion Date	Enter the completion date of the plan.
Information SSP Approval Date	Enter the date the SSP was approved, and indicate whether the approval documentation is attached or is on file.
Prior Self-Assessments	Append the four most recent SP self-assessments as described in Section 4.1.

2.2.1 SP Management Authorization of SSP

Senior SP management must authorize the SSP. Management authorization shall be based on an assessment of management, operational and technical controls. Moreover, because the SSP establishes and documents the security controls, it should form the basis for the authorization, supplemented by the assessment report and a plan of actions and milestones. A plan of actions and milestones submitted by the information system owner is used to monitor progress in correcting deficiencies noted during the security assessment. By authorizing processing in a system, the manager accepts its associated risk.

2.2.2 SSP Reauthorization

Reauthorization of the SSP by senior SP management shall occur whenever there is a significant change in processing, or at least every 12 months.

3. Enrollment/Verification Process Standards

Enrollment/Verification Process Standards provide process-specific guidelines for establishing internal controls over the following enrollment and verification processes:

- Privacy protection;
- EP and VP employee training;
- Personnel security;
- Enrollment support, eligibility, forms;
- Acceptable U.S. government-issued identification documents;
- Information provided to RT applicants at enrollment and permissions on other uses of information;
- Biographic and biometric data collection;
- Credentialing;
- Notification of eligibility;
- Enrollment/verification; and
- Incident reporting.

The SE/SP shall assume all costs related to the described responsibilities to conduct RT operations, including services, equipment, personnel, facilities and removal of all equipment and related materials if RT operations are terminated at a site. SPs shall provide equal access to prospective RT applicants with disabilities and adhere to any applicable Section 508 requirements of the Rehabilitation Act.

Upon expiration or termination of a contract with an SP, the SE shall require any substitute SP to maintain all obligations of privacy, security and data retention requirements imposed upon such information by TSA and all promises of privacy and security made to RT Participants by the SP, provided such promises and obligations have been delivered to the SE in writing.

Table 3-1, Enrollment/Verification Security Control Standards, provides an overview of enrollment/verification processes and their corresponding security control standards.

Table 3-1. Enrollment/Verification Security Control Standards

Enrollment/Verification Processes	Standards
Acceptable U.S. Government-Issued Identification Documents	• Acceptable documents will be identified from a list based on Federal Form I-9. • Two enrollment technicians shall validate an applicant's identification documentation independently. • SP shall use a front-end validation device or other document authentication technologies for antifraud features.
Biographic and Biometric Data Collection	• The following biographic information shall be requested from RT applicants at enrollment in order for TSA to conduct and adjudicate a name-based security threat assessment: full legal name (as listed on the government-issued identity documents used to establish identity), other names used (such as maiden name or alias), Social Security Number (optional), citizenship status, Alien Registration Number (if applicable), current home address (P.O. Box will not be accepted), primary and secondary telephone numbers (home, work or cellular), current e-mail address, date of birth, place of birth, gender and height. • The SE/SP shall capture the required biometric information in accordance with the RTIC Technical Interoperability Specification.
Credentialing	• The RT card shall adhere to the RTIC Technical Interoperability Specification. • The back of the RT card must state that it is not a federal ID. • The RT card shall include a shared secret. • The RT card should survive normal wear and tear.
EP Employee Training	• The EP shall develop and conduct comprehensive training for all EP employees that covers at a minimum: – Sessions on all policies, privacy and security of applicant personal information; – User identification and authorization requirements; – Use of the biometric software and capture device to obtain an acceptable user image; – Identification of an unacceptable image that needs to be recaptured; – Recapturing of an image when there is an indication that the image has not been properly captured; and – Enrollment customer service activities.
Enrollment Support, Eligibility, Forms	• The SE/SP shall provide enrollment support to RT applicants and participants. • The SE/SP shall accept applications from persons self-identifying as U.S. citizens, U.S. nationals and lawful permanent residents of the United States.

Enrollment/Verification Processes	Standards
Enrollment/Verification	• The SE/SP will acquire and install all necessary biometric sensors, software, licenses and any other necessary services required to operate verification stations that comport with the information systems standards set forth in this document. • The SE will make available RT lines at locations jointly decided by the SE and TSA. The decision will consider whether there will be adverse effects on either throughput or wait times at any of the other lines or lanes. • The SE/SP may not refuse service to an RT Participant regardless of the SE/SP with whom that person enrolled, as long as the SP has been approved by TSA to provide RT services.
Incident Reporting	• In the event of a security incident, SPs must provide incident reports to various key RT stakeholders, such as the SE, the CIMS Information System Security Officer (ISSO) and the RT Program Management Office (PMO). This section provides the security incident reporting requirements with respect to the RT PMO specifically. This section does not preempt any additional reporting requirements that SPs may be legally or contractually obligated to execute with respect to other entities.
Information Provided to RT Applicants at Enrollment and Permissions on Other Uses of Information	• The SE/SP shall provide each RT applicant with a TSA Privacy Act Statement. • The SE/SP shall provide each RT applicant with the ability to opt-in to non-RT benefits, if offered. If such an opt-in requires the collection of data beyond that required for RT, the SE/SP shall ensure that the RT applicant expressly authorizes the opt-in (e.g., selecting a checkbox for online enrollment). • The SE/SP also shall ensure that there is a logical separation between such additional information and the base RT enrollment screen/form (e.g., separate screen). The SE/SP shall state clearly that the collection of such additional information is neither required nor endorsed by TSA. • The SE/SP shall not collect the additional biographic data or any other information on the RT enrollment form, nor shall the RT enrollment form capture the opt-in declaration from the application. • The mechanisms for capturing the opt-in declaration from the applicant and the subsequent collection of the applicant's information are described in Section 3.4.6.1.
Notification of Eligibility	• The SP shall notify the individual that his or her registration in RT has been confirmed and that he or she has been approved to participate in RT. • The SP is not responsible for notifying RT applicants of a "not approved" TSA security threat assessment. The responsibility to notify the applicant directly rests solely with TSA.
Personnel Security	• SPs are required to submit biographic information and fingerprints of all key personnel for a CHRC and security threat assessment.
Privacy Protection	• SPs must establish a written privacy policy, in accordance with the Fair Information Practice Principles, to govern the data collected in connection with RT and will be required to provide this policy, in writing, to each eligible RT applicant. • In addition, the SP must provide each eligible RT applicant, at the time of enrollment, with a copy of the Privacy Act Statement supplied by TSA.

Enrollment/Verification Processes	Standards
VP Employee Training	• The VP shall develop and conduct comprehensive training for all VP employees covering, at a minimum: – Understanding the false acceptance rate and false rejection rate configurations as outlined in Section 3.4.9; – Configuring the biometric system to prohibit an identical biometric sample from being used in authentication attempts, after the maximum of three attempts per biometric has been reached; – Verification process threat awareness identification and reporting; – Fallback procedures whenever the verification process cannot be used (in accordance with Control VP-5, Fallback Controls, in Appendix C); – Verification station operations.

3.1 Privacy Protection

SPs shall establish a written privacy policy to govern the data collected in connection with the RT Program and shall be required to provide this policy, in writing, to each eligible RT applicant. At a minimum, SPs should follow the Fair Information Practice Principles in developing their privacy policy. Table 3-2, Fair Information Practice Principles, provides an overview of the standard. In addition, the SP shall provide each eligible RT applicant, at the time of enrollment, with a copy of the Privacy Act Statement supplied by TSA (see Section 3.4.5). SPs also shall review their privacy policy during the annual self-assessment. SEs and SPs may adopt privacy policies that are more stringent than required by TSA; however, they may not withhold information requested by TSA.

Table 3-2. Fair Information Practice Principles

#	Principle	Description
1.	Openness	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
2.	Collection Limitation	There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
3.	Purpose Specification	The purpose for which personal data is collected should be specified not later than at the time of data collection, and the subsequent use should be limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

#	Principle	Description
4.	Use Limitation	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified above, except with the consent of the data subject or by the authority of law.
5.	Data Quality	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, relevant and kept up to date.
6.	Individual Participation	An individual should have the right to: (1) obtain from a data controller, or otherwise, confirmation of whether the data controller has data relating to him/her; (2) have communicated to him data relating to him/her within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner and in a form that is readily intelligible to him/her; (3) be given reasons if a request is denied and be able to challenge such denial; and (d) challenge data relating to him/her and, if the challenge is successful, to have the data erased, rectified, completed or amended.
7.	Security Safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
8.	Accountability	A data controller should be accountable for complying with measures which give effect to the principles stated above.

The SE is responsible for ensuring that the SPs maintain, use and retain applicant and participant biographic and biometric data necessary for RT operation in accordance with the SP's privacy policy. Enrollment information will be transmitted by the SP using the Triple Data Encryption Standard.[1]

The SE/SP shall retain an individual's personal information only to the extent necessary to provide customer service, unless the individual grants permission to collect and retain that information. (See Section 3.4.6.)

3.2 Training

The SE shall develop and conduct a comprehensive training program for all employees who perform RT functions (e.g., customer service personnel, enrollment and verification personnel, system administrators). The training program will include sessions on all polices and procedures, including privacy and security of RT applicant/participant personal information, security, effective customer service, enrollment functions, verification processes and employee services information. Any training will be consistent with agreements between TSA and the SE, including ASP/AOSSP/MSPs and MOU/MOAs. The SE will ensure that employees abide by the policies and standards set forth in this document, the SE plan of operations and other applicable documents.

[1] The Triple Data Encryption Standard is an approved cryptographic algorithm as required by FIPS 140-2, Security Requirements for Cryptographic Modules.

3.3 Personnel Security

3.3.1 Initial Submission of SP Key Personnel

As part of the initial application process to become an approved SP in the RT Program, SPs are required to submit biographic information and fingerprints of all key officers (as listed in the first two bullets below) for a CHRC and a security threat assessment. Key personnel must be U.S. citizens, nationals or lawful permanent residents and must pass both the CHRC and security threat assessment. The CHRC and security threat assessment involve checks against government databases to determine whether an individual is a threat to transportation or national security.

Key personnel include:

- Company officers/principals/directors with direct authority over RT Program operations;
- Key officers/principals/directors of primary subcontractors and/or business partners with direct authority over RT Program operations; and
- Employees with access to PII or RT software and equipment.

The SP Security Officer submits the following biographic information for each of the SP key personnel into the Regulated Party Online Background Operations and Tracking System (ROBOTS), a secure, web-based application:

- Full legal name (as listed on government-issued identity documents);
- Date of birth; and
- Last four digits of the person's Social Security Number (optional).

The SP Security Officer creates personal user accounts for each of the SP key personnel. Key personnel then are instructed to log in and update their records with additional biographical information.

The fingerprint submission takes place at the SP's local airport or other approved location and is arranged in coordination with a TSA Security Manager. TSA will provide detailed procedures and forms to SPs to facilitate the key personnel submission and communication process.

3.3.2 Addition of Key Personnel After Approval

Once an SP has been approved and is operational, biographic information and fingerprints of new key personnel must be submitted to TSA for a CHRC and security threat assessment. SPs may not allow any personnel to perform RT functions as defined in Section 3.2 until those individuals have passed the TSA CHRC and security threat assessment vetting process.

3.3.3 Updates to Key Personnel Information After Approval

If any key personnel changes his or her full legal name or needs to correct any other biographic information, the information shall be resubmitted to TSA for a reassessment of security status. The SP shall collect and submit biographic data updates within 30 days of any change.

3.3.4 Removal of Key Personnel After Approval

SPs shall notify the RT PMO of any departures of key personnel within 10 business days of the individual's departure. This will enable TSA to remove the individual from the perpetual security vetting process. TSA will provide approved SPs forms and procedures for submitting notifications of departures.

3.3.5 Receipt and Management of Results

The RT PMO will provide regular personnel status updates to each SP, which will inform the SP of the status of each individual submitted (e.g., approved, in process, or not approved). Each SP shall maintain accurate and up-to-date CHRC and security threat assessment results for its key personnel.

In any case where key personnel or an employee receives a "not approved" status, the RT PMO will advise the SP directly of this status via the SP Personnel Status Report. The SP is responsible for handling this information in accordance with its corporate human resources and privacy policies, as well as all applicable federal or state regulations. (Note: This requirement differs from the usual process for notifications of "not approved" for RT applicants, as described in Section 3.4.12. For typical RT applicants, the responsibility to notify an applicant of "not approved" status rests solely with TSA.)

3.3.6 Periodic Reconciliation with TSA

On a periodic basis (every 6 months or more frequently if needed), SPs will be required to submit a list of key personnel. This will enable TSA to ensure its records are consistent with SP records and to resolve any data inconsistencies. SPs are required to submit this list within five business days of receipt of a request from TSA.

3.4 Enrollment Standards

3.4.1 Support

The SE/SP shall provide enrollment support to RT applicants and participants. This support may include:

- Assistance in the completion of online pre-enrollment forms;
- In-person enrollment using enrollment stations and processes that meet the RTIC Technical Interoperability Specification;
- Identity document verification;
- Biometric image capture; and
- Customer service.

TSA may require the SE/SP to revise marketing materials if TSA determines that these materials contain erroneous or misleading information about the RT Program.

3.4.2 Enrollment Eligibility

The SE/SP may permit only persons meeting TSA's requirements for this program to enroll. Only TSA will conduct security threat assessments.

The SE/SP shall accept applications from applicants who provide proof of identity and proof that they are citizens, U.S. nationals or lawful permanent residents of the United States. (See Section 3.4.4.) If an agent determines that a document is fraudulent, the agent shall return the document to the applicant and deny the application.

3.4.3 Enrollment Forms

The SE/SP shall not collect any excess data (as defined in Section 3.4.6.1) directly on the RT enrollment form or screen. Any excess data shall be collected on separate forms. The SE/SP shall not transmit or share any excess data with TSA.

The SP shall maintain an archived electronic copy of the completed enrollment form, in accordance with its written privacy policy and the Privacy Act. (See Section 3.1, Privacy Protection.) Copies shall be made available to TSA upon request.

3.4.4 Acceptable Documents to Establish Identity and Eligibility

In order to participate in the RT Program, each RT applicant must present two documents to establish identity and eligibility to the EP. TSA has established a list of acceptable documents that will be used to satisfy these requirements. This list is based on Federal Form I-9.[2]

One document must be a government-issued photo ID, one must contain security features capable of being verified through authentication technology and one must confirm that the applicant is a U.S. citizen, a U.S. national or a lawful permanent resident of the United States. If a single document meets all of these requirements, a second document from the list still is required. Table 3-3, Acceptable Identity and Eligibility Documents, lists the options for meeting these requirements. SPs shall verify participant identity and eligibility by validating two forms of identification, at least one of which must be verified using document authentication technologies. SPs shall verify the identity documents using a front-end validation device or other document authentication technologies that take advantage of antifraud features incorporated into government-issued identification documents. High-resolution digital images of all identity documentation will be captured and stored in a secure database using the Advanced Encryption Standard.[3]

[2] The RT Program narrowed the list of acceptable documents to a subset of the Federal Form I-9 list.

[3] The Advanced Encryption Standard specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data.

Table 3-3. Acceptable Identity and Eligibility Documents

Documents That Establish U.S. Citizenship, Status as a U.S. National, or U.S. Permanent Residency	Documents That Establish Identity	Documents That Contain Security Features Capable of Being Verified Through Authentication Technology
• U.S. passport (Unexpired or expired) • Certificate of Citizenship (Form N-560 or N-561) • Certificate of Naturalization (Form N-550 or N-570) • Valid U.S.-issued Permanent Resident Card or Alien Registration Receipt Card with photograph • Original or certified copy of U.S. birth certificate • Certificate of Birth Abroad issued by the U.S. Department of State (Form FS-545 or Form DS-1350)	• U.S. passport (Unexpired or expired) • Certificate of Citizenship (Form N-560 or N-561) • Certificate of Naturalization (Form N-550 or N-570) • State-issued driver's license or ID card issued by a state or outlying possession of the United States, provided that it contains a photograph and information such as name, date of birth, gender, height, eye color and address • U.S. military ID card or DD Form 214, Certificate of Release or Discharge From Active Duty • Foreign passport (Unexpired)	• U.S. passport (Unexpired or expired) • State-issued driver's license or ID card issued by a state or outlying possession of the United States, provided that it contains a photograph and information such as name, date of birth, gender, height, eye color and address, and provided that the state or possession has not declared the license or ID card invalid for identification purposes by the federal government[4] • Foreign passport (Unexpired)[5] • U.S. military ID card (Unexpired)

The following are the possible combinations of documents that can be used to fulfill RT identification and eligibility requirements:

1. An expired or unexpired U.S. passport AND any one of the following:
   - Certificate of Citizenship (Form N-560 or N-561);
   - Certificate of Naturalization (Form N-550 or N-570);
   - Valid U.S.-issued Permanent Resident Card or Alien Registration Receipt Card with photograph;
   - Original or certified copy of U.S. birth certificate;
   - Certificate of Birth Abroad issued by the U.S. Department of State (Form FS-545 or Form DS-1350);
   - Foreign passport (unexpired);

[4] Not all driver's licenses or ID cards issued by states and possessions contain security features capable of being authenticated via technology. Only individuals from states and possessions that issue IDs or driver's licenses with these security features may submit this document in order to meet the identity requirements. As an alternative, a U.S. passport or unexpired foreign passport with these features may be submitted to fulfill the requirement.

[5] All foreign passports do not have this capability. Only passports that can be authenticated using technology can be presented to satisfy this requirement.

- State-issued driver's license or ID card issued by a state or outlying possession of the United States, provided that the license or ID card contains a photograph and information such as name, date of birth, gender, height, eye color and address; and
- U.S. military ID card or DD Form 214, Certificate of Release or Discharge From Active Duty.

2. A State-issued driver's license or ID card issued by a state or outlying possession of the United States, provided that the license or ID card contains a photograph; information such as name, date of birth, gender, height, eye color and address; and security features capable of being verified through authentication technology, and provided the state or possession has not declared the license or ID card invalid for identification purposes by the federal government, AND any one of the following:
   - Certificate of Citizenship (Form N-560 or N-561);
   - Certificate of Naturalization (Form N-550 or N-570);
   - Valid U.S.-issued Permanent Resident Card or Alien Registration Receipt Card with photograph;
   - Original or certified copy of U.S. birth certificate; and
   - Certificate of Birth Abroad issued by the U.S. Department of State (Form FS-545 or Form DS-1350).
3. An unexpired foreign passport that contains security features capable of being verified through authentication technology AND any one of the following:
   - Certificate of Citizenship (Form N-560 or N-561);
   - Certificate of Naturalization (Form N-550 or N-570); and
   - Valid U.S.-issued Permanent Resident Card or Alien Registration Receipt Card with photograph.
4. A military ID card issued by the U.S. Department of Defense, provided it contains a photograph, information such as name and date of birth and security features capable of being verified through authentication technology, and provided that the ID card has not been declared invalid for identification purposes by the federal government, AND any one of the following:
   - Certificate of Citizenship (Form N-560 or N-561);
   - Certificate of Naturalization (Form N-550 or N-570);
   - Valid U.S.-issued Permanent Resident Card or Alien Registration Receipt Card with photograph;
   - Original or certified copy of U.S. birth certificate; and
   - Certificate of Birth Abroad issued by the U.S. Department of State (Form FS-545 or Form DS-1350).

If the RT applicant chooses to use a U.S. passport to establish identity, using it likely will expedite the security threat assessment process because U.S. passports are well suited to assist in adjudicating cases.

If the RT applicant submits breeder documents with differing surnames (i.e., married and maiden names) for the purpose of confirming identity or citizenship/immigration status, the SP will submit both of the applicant's surnames for TSA review.

Two enrollment technicians independently shall validate an applicant's identification documentation. The enrollment system shall capture a unique identifier using a digital signature for each authorizing technician. SPs shall verify operator

identity based on 1:1 biometric verification for every enrollment, pass the operator identifier to the CIMS and ensure chain-of-trust from a component level with digital signatures and encryption of the enrollment message.

3.4.5 Information Provided to Applicant at Enrollment

The SE/SP shall provide each RT applicant with the following written statement at the time of application:

TSA Privacy Act Statement

Authority: 49 U.S.C. 114 authorizes collection of this information.

Purpose: TSA is collecting this information from all individuals who apply to participate in the Registered Traveler program. TSA will use this information to verify your identity; to conduct and adjudicate a security threat assessment; if you are accepted into the Registered Traveler program, to conduct ongoing security threat assessments; and to issue a "smart card" to you that will identify you as a Registered Traveler. Furnishing this information is voluntary. However, failure to provide it may delay or prevent the completion of the security threat assessment, without which you may not be permitted to participate in this program.

Routine Uses: The information will be used by and disclosed to TSA personnel and contractors or other agents who need the information to assist in the operation of the Registered Traveler program. Additionally, TSA may share this information with airports and airlines to the extent necessary to ensure proper identification, ticketing, security screening and boarding of Registered Travelers. TSA may disclose information to appropriate law enforcement or other government agencies as necessary to identify and respond to outstanding criminal warrants or potential threats to transportation security. TSA also may disclose information pursuant to its published system of records notices, DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS) and DHS/TSA 015, Registered Traveler Operations Files, both of which were last published in the Federal Register on November 8, 2005, at 70 FR 67731-67736.

Web-based interfaces shall require applicants to select an "acknowledgement" radio button or checkbox indicating that they have read and understand the statement. At that point, web applicants may "click through" the page displaying the statement.

In addition, the SE/SP shall inform each person who volunteers to participate in the RT Program, in writing, that:

1. The RT Program is linked to the national security environment, and TSA can suspend the program at any or all locations at any time if changes in the security environment warrant.
2. Payment of a fee to participate in the RT Program neither guarantees acceptance in the program nor continued enrollment status.
3. If the SE/SP collects any additional biographic, biometric or billing information not required by TSA for participation in the RT Program (the excess data), the SP shall:

   a) Inform the applicant in writing that:

      i. Collection of the excess data is neither required nor endorsed by TSA;

      ii. The excess data is collected for SE and SP use only and not for TSA use; and

      iii. Provision of the excess data to the SP is not required for participation in the RT Program.

   b) Ensure that there is a logical separation between the collection of such additional information and the base RT enrollment screen/form (e.g., separate screen).

   c) Ensure the applicant expressly authorizes the collection of excess data.

4. Iris images may be shared with NIST for purposes of research to develop government standards for the use of iris images. Iris images will be shared with NIST only after TSA enters into an MOU to minimize privacy impacts and secure the data. Participation is strictly voluntary, and individuals will opt-in separately to share images with NIST for future research purposes.

All SPs must include a Paperwork Reduction Act (PRA) Statement of Public Burden on their web sites. The Paperwork Reduction Act (PRA) of 1995 requires federal agencies to seek and obtain approval from the Office of Management and Budget (OMB) before undertaking a collection of information directed to 10 or more persons. The PRA tasks OMB, which is part of the executive branch of the federal government, with reviewing and approving proposed agency information collections. TSA has sought and obtained OMB approval for the collection of information that is a part of the RT Program. One of these collections is the enrollment of RT Program participants. Although TSA does not conduct this collection directly, under the PRA, TSA is considered to be "sponsoring" the collection because TSA is requiring SPs to collect minimum identifying information, which is necessary for TSA to conduct a security threat assessment on the applicant.

The PRA requires each agency to display a currently valid OMB control number and inform respondents that a response is not required unless the collection of information displays a valid OMB control number on each collection of information. This information is relayed to respondents in a PRA Statement of Public Burden that must be displayed on the face of the collection instrument, which in this case is the enrollment screen where SPs solicit the information TSA is requesting. (Note: The application an RT SP completed to become an RT SP also contained a Statement of Public Burden in compliance with the PRA.) Although TSA has offered to display the Statement of Public Burden on its RT web site to comply with these requirements, OMB nonetheless is requiring that to comply with the PRA, SPs prominently display the following Statement of Public Burden, at minimum, on the first screen of the RT enrollment form or on a screen immediately preceding that screen. As such, the following statement must be displayed:

Paperwork Reduction Act Statement of Public Burden:

TSA requires a full legal name from RT Program applicants for the purpose of conducting a security threat assessment. TSA also requests the following identifying information: other names used, Social Security Number, citizenship status, Alien Registration Number, current home address, primary and secondary telephone numbers, current e-mail address, date of birth, place of birth, gender, height, previous home addresses, employer name, employer address and driver's license number. TSA will use this information for the following purposes: to prescreen travelers by conducting security threat assessments, to assist in the management and tracking of security threat assessment results, to permit the retrieval of security threat assessment results, to eliminate false watch list matches, to communicate with the individual in the event of a possible match and to refer to the appropriate intelligence and law enforcement entities the identity of RT applicants or RT Participants who pose or are suspected of posing a threat to transportation or national security.

The identifying information requested by TSA is a voluntary collection, but failure to provide this information may delay or prevent an "approved" determination of the security threat assessment necessary to join RT. Participating Service Providers (SPs) may collect additional information from you for customer service purposes. The collection of excess data by SPs is neither required nor endorsed by TSA.

TSA estimates that the total average burden per response associated with this collection is approximately 20 minutes. If you wish to comment on the accuracy of that estimate or submit suggestions for reducing the burden, you may write to TSA, Registered Traveler Program, 601 S. 12th St., Arlington, VA 22202-4220. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The OMB control number assigned to this collection is 1652-0019.

3.4.6 Permissions on Other Uses of Information

The SP shall obtain and retain an explicit digital or physical signature from applicants giving their consent to the following:

1. TSA or its agents transmitting an "approved" or "not approved" determination of the applicant's TSA security threat assessment directly to the SP. TSA or its agents will not transmit the content of the TSA security threat assessment nor the reason behind the "approved" or "not approved" determination.

2. The SP may collect, retain and use excess data (as set forth in Section 3.4.6.1). For paper enrollments, the separate agreements shall be in the form of separate sheets of paper, describing the consent being provided, and shall be signed in writing by the applicant.

   For web-based enrollments, the separate agreements shall be in the form of unique web pages, each requiring the selection of a radio button or checkbox, stating that the applicant, by selecting the item, acknowledges consent to the action. All such web pages shall have a "cancel" option which permits navigation away from, or closing of, that page.

3.4.6.1 Collection and Use of Excess Data

1. The SE/SP may elect to solicit the applicant, at the time the applicant is presented with the RT enrollment form (either analog [paper] or digital [web-based]), for permission to capture RT applicant information (called excess data) for use in programs that are not related to RT (non-RT benefits). Such solicitation may not be collected on the RT applicant form, nor may a checkbox or other similar mechanism be used to collect intent to opt-in by the applicant for participation in non-RT benefits. If the applicant does not opt-in to provide excess data and participate in non-RT benefits, the SE/SP may not use any of the applicant's information for any purpose other than the support of the RT Program.

2. If the SE/SP collects any additional biographic, biometric or billing information not required by TSA for participation in RT (the excess data), the SE/SP shall inform the applicant in writing (either paper or web-based) that:

   a) Collection of the excess data is neither required nor endorsed by TSA;

   b) The excess data is being collected for SE and/or SP use only and not for TSA use;

   c) The provision of the excess data to the SP is not required for participation in the RT Program and will have no impact on the processing time or final eligibility determination made by TSA; and

   d) The applicant may, after electing to participate in non-RT benefits, withdraw permission at a later time, and the SE/SP shall provide clear instructions describing how to do so.

3. Solicitations for excess data and/or participation in non-RT benefits must be marked conspicuously with the name, brand, logo or identifying language of the SE/SP. Government logos, brands, organization names or program names may not appear anywhere on these solicitations. The relationship between the solicitation and TSA or the RT Program shall be clarified such that reasonable applicants would not assume incorrectly that the solicitations are part of their RT applications.

4. For paper applications, the SE/SP may include detached solicitations in the form of sheets of paper, brochures or pamphlets. The information may be collected on the spot, or the SE/SP may offer the option of mailing the materials to the SE/SP at a later time. Each solicitation must collect the applicant's signature acknowledging items 2.a through 2.d above.

5. For web-based applications, the SE/SP may place a link, button or other conspicuous navigational item that triggers a link to the solicitation material. Prior to navigating to this material, an intermediate page, containing items 2.a through 2.d above, shall be presented. Applicants must acknowledge they have read and understand this information

by selecting a radio button, checkbox or similar mechanism, and then "clicking through" to arrive at the solicitation material. A "cancel" button also shall be present and, when selected, will end the solicitation process. Web-based systems will not employ pop-up or pop-under ads, nor will they use spyware (software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user) while on RT application screens. Cookies are permitted, but they must not persist from one session to another and may be created and retrieved only by the SP/EP web server.

3.4.7 Biographic Data Collection

The following biographic information shall be requested from RT applicants at enrollment in order for TSA to conduct and adjudicate a name-based security threat assessment: full legal name (as listed on the government-issued identity documents used to establish identity), other names used (such as maiden name or alias), Social Security Number (optional), citizenship status, Alien Registration Number (if applicable), current home address (P.O. Box will not be accepted), primary and secondary telephone numbers (home, work or cellular), current e-mail address, date of birth, place of birth, gender and height. Provision of the requested information, including Social Security Number, is voluntary. However, failure to provide all of the requested biographic information may delay or prevent an "approved" determination of the security threat assessment necessary to join the RT Program.

The following are optional but may facilitate adjudication: prior home addresses (for the past 5 years), driver's license number and state of issuance and employer's name and address.

The SE/SP may develop a GUI-based enrollment application to collect and store the volunteered data. The GUI application shall be user-friendly and use industry standard data entry form features such as list of values, radio buttons, field validation and mandatory fields. All fields will comply with the formats outlined in the ISA/MOU/MOA established by the CIMS system owner and the SP.

SPs shall establish authorization procedures that verify the accuracy of a participant's biographic data through the use of field-level edit checks within enrollment systems. Additionally, applicants must be able to verify and confirm their biographic data prior to submission to TSA.

SPs shall establish the capability for applicants and approved participants to update their biographical data when changes occur and/or on an annual basis.

3.4.8 Update of Participant Biographic Data

The RT Participant may change or update biographic data. Changes could be due to relocation or marriage, affecting contact information or name change. Updates to participant data also may occur to correct errors.

Some changes in participant biographic data may require re-evaluation of the participant's security threat assessment status. The SE/SP shall attempt to collect participant biographic data updates within 30 days of any change but in all cases shall collect updated biographic data from participants on an annual basis.

The SE/SP shall reverify participant identity documents and recapture digital images of participant identity documents, as specified in Section 3.4.4, whenever a participant reports changes or updates to any of the following biographic information to the SE/SP:

- Name;
- Gender;
- Date of birth;
- Citizenship status;
- Place of birth;
- Social Security Number;
- Alien Registration Number;
- Driver's license number and state;
- Passport type; and
- Passport number.

3.4.9 Biometric Data Collection

The SE/SP shall capture the required biometric information in accordance with the RTIC Technical Interoperability Specification.

Biometric images must be captured at enrollment, and data must be maintained in a secure format. The enrollment system also shall capture an operator identifier upon a 1:1 verification to identify the technician and digitally sign the enrollment message to protect the data from tampering. SPs shall ensure that enrollment technicians are trained appropriately in the collection of biometric data.

The SE/SP enrollment system must meet or exceed all biometric quality requirements set forth in the RTIC Technical Interoperability Specification. Biometric enrollment hardware and software must be able to verify the success of the enrollment process, including the ability to provide such enrollment metrics as quality of fingerprint or iris images captured.

Ten print images, if available, must be captured at enrollment in a manner consistent with the RTIC Technical Interoperability Specification. If an individual applicant does not have 10 digits but has at least four digits, then the SE/SP shall capture the images associated with as many digits as possible. If an individual has fewer than four quality fingerprints, the SE/SP shall contact the TSA RT PMO for waiver submission procedures.

The biometric devices used must be able to achieve a false reject rate of 1 percent or less and a false acceptance rate of 1 percent or less with a verification policy allowing three attempts to verify on any two unique biometrics stored on the RT card.

The SE/SP must be able to collect iris images at enrollment in a manner consistent with the RTIC Technical Interoperability Specification. The provision of iris images is at the discretion of the applicant, and the SE/SP may not require that the enrollee provide iris images. If the enrollee chooses to provide iris images, images of two irises (both the left and right iris), if available, will be taken and used for identity verification purposes.

If TSA requires the collection of other biometric information at a later date in accordance with any new TSA or U.S. Department of Homeland Security policies and guidelines, the SE/SP will modify its systems as updated standards require.

3.4.10 Separation of Biographic and Biometric Information

All database systems used in the RT Program shall be designed to separate the storage of biometric and biographic data in distinct logical databases. Privileges to access data in these databases also shall be separated such that the ability for a single individual to access both biographic and biometric data can be restricted. Indexing of the biometric database shall not be able to be related in any way with the personal identity associated with the biometrics. Biometric and biographic data within RT database systems shall be encrypted at rest with a minimum strength of AES FIPS 140-2 validated cryptography. Key generation, key replacement and other aspects of key management shall be explained in the SSPs.

3.4.11 Credential

The SE/SP shall issue RT cards to individuals with "approved" TSA security threat assessment determinations after those individuals are accepted into the RT Program. The SE/SP will issue and replace RT cards, as necessary, informing the CIMS of the need to issue replacements. The cards shall adhere to the RTIC Technical Interoperability Specification. Any credentialing solution and the technology it houses shall survive normal wear and tear consistent with applicable International Organization for Standardization standards and industry best practices. SPs may add additional information to the card but cannot add information to the RT Program applet on the card or access or use the information on that applet in any manner that violates the established standards for the RT Program, including all privacy protection standards.

Additionally, the back of the RT card shall state the following: "This is not a government identification card."

A user's private information stored in his or her card shall be stored in a protected state while at rest (the card is disengaged from a valid verification station). A secret key (KC) shall be used to restrict access to the private authentication data, using the Triple Data Encryption Standard. The RT card will not reveal the private information until the authentication protocol succeeds at the verification station and with the Hardware Security Module (HSM) that holds the master secret.

In the event that the KC is compromised (for example, the RT card is lost or stolen), a new card shall be provided to the RT Participant. This card will utilize a new KC to protect the private information on the card while it is disengaged from the verification station.

Reports of lost or stolen cards, or reports that a KC may have been compromised, shall be reported by the SP via more than one channel, with at least one channel being a telephone call. Upon receipt of such a report, the SP must notify the CIMS electronically. The CIMS will propagate the report to parties with a need to know and will process the card for inclusion on the revocation lists.

3.4.12 Notification of Eligibility

Once an applicant is determined by TSA to be eligible to participate in the RT Program, the SP shall communicate a notification, by first class letter via the United States Postal Service (USPS), to the individual stating that his or her registration in the RT Program has been confirmed and that he or she has been approved to participate in the RT Program. Mailing the notification via USPS validates the applicant's listed address and is the most reliable method to send communication. (The SP is not responsible for notifying RT applicants of a "not approved" TSA security threat assessment. The responsibility to notify the applicant rests with TSA.)

The SP shall develop a process allowing for the daily processing of all newly updated RT Participant status files from the CIMS. SPs shall notify the CIMS within 24 hours when a card should be deactivated (when lost, stolen or malfunctioning).

3.5 Verification Standards

3.5.1 Verification Station Operations

The SE/SP shall acquire and install all necessary iris and fingerprint biometric sensors, software, licenses and any other necessary services required to operate verification stations that comply with the information system security standards set forth in this document.

The SE/SP shall use the most recent RT status results (including the current TSA security threat assessment findings and other eligibility-determining factors) provided by the CIMS. A current Card Revocation List (CRL) is maintained within the CIMS and is provided to VPs on a regular basis (every 12 hours) or upon request. VPs are responsible for propagating CRLs received from the CIMS to all of their verification stations. It is anticipated that such propagation should take minutes only; however, it is required to occur within six hours of receipt from the CIMS to accommodate airport operations and offline verification stations. If a verification station has not received an update from the CIMS within 24 hours, it must cease to accept RT Participant verification requests, because the station may not have the latest CRL.

The SE/SP shall conduct biometric matching of each RT Participant at the verification station and shall ensure that identity verification is confirmed prior to permitting the individual to enter a screening checkpoint as an RT Participant. This biometric verification will be accomplished as outlined in the RTIC Technical Interoperability Specification and will not have a negative impact on checkpoint security throughput. SPs must retain this information in accordance with information systems security standards outlined in Appendix C at System and Information Integrity (SI)-12 Information Output, Handling and Retention.

The SE/SP shall ensure that the traveler's name on the government-issued photo identification matches the name on the boarding pass. The SE/SP shall ensure that all individuals who present themselves as RT Participants have an acceptable biometric match prior to entering the screening checkpoint. RT Participants will be allowed a maximum of three attempts to authenticate using their primary biometric, followed by three attempts to authenticate using a secondary biometric. Those individuals not confirmed by the verification station (for any reason, including the verification station not working properly) will not be allowed to use RT lines or lanes. The SP will direct unconfirmed travelers to be screened in the same manner as nonparticipants.

The verification HSM and associated activation card shall be designed to protect the shared secrets in use by the RT cryptographic algorithm. In the event that a verification station, with an HSM and its associated activation card, is lost or stolen, or the shared secret is compromised, the SE will employ the SP to notify the CIMS, which will in turn notify TSA and SPs. TSA will conduct a risk assessment to develop an appropriate mitigating response. As discussed in the RTIC Technical Interoperability Specification, this response may include notification of RT Participants that their card potentially is at risk of being accessed without their consent if it is lost or stolen. SPs are responsible for notifying their own members of this event and will be required to offer members a new card, at no cost to the participant.

3.5.2 Location of Verification Stations

The SE will make available RT lines at locations jointly decided by the SE and TSA. The decision will consider whether the potential location will have adverse effects on either throughput or wait times at any of the other lines or lanes.

3.5.3 Interoperability

The SE/SP may not refuse service to an RT Participant regardless of the SE/SP with whom that person enrolled, provided the EP is approved by TSA to provide RT services. The SE/SP will allow such a person to use RT lines and lanes at no additional cost to the participant.

3.6 Incident Reporting

In the event of a security incident, SPs must provide incident reports to various key RT stakeholders, such as the SE, the CIMS ISSO and the RT PMO. This section provides security incident reporting requirements with respect to the RT PMO. This section does not preempt any *additional* reporting requirements that SPs may be legally or contractually obligated to execute with respect to other entities.

The majority of security incidents will be minor in nature (e.g., a successful quarantine of a virus by antivirus software) and do not need to be reported to the RT PMO. However, more serious incidents must be reported to the RT PMO within a defined time period. These incidents are grouped into two categories:

- Privacy incident; and
- Loss of availability.

SPs may use their own incident reporting processes and forms, but at a minimum should report:

- Date/time;
- Location;
- Affected systems;
- Type of incident; and
- Expected recovery time.

3.6.1 Privacy Incident

A privacy incident is defined as any loss of control, compromise, unauthorized disclosure, acquisition, access or any similar term referring to situations where unauthorized users, or for an unauthorized purpose, have access or potential access to PII in usable form, whether physical or electronic. Potentially, an incident of this nature could allow for disclosure, identity fraud, lawsuit and reduced public confidence in the RT Program. Examples of privacy incidents include:

- Lost or stolen data storage device;
- Suspected or confirmed unauthorized access to data; and
- Unauthorized access to paperwork that contains the names, Social Security Numbers, dates of birth and/or fingerprints of employees.

In addition to meeting reporting requirements of existing contracts, an incident of this type should be reported to the RT Information Security Manager within one hour of discovery via the e-mail address: **RT.Security@tsa.dhs.gov**.

3.6.2 Loss of Availability

A loss of availability incident is defined as any loss of access to or use of RT verification stations, during normal hours of operation, for longer than one hour. Potentially, an incident of this nature could allow for reduced public confidence in the RT Program and reduced public utilization of the RT Program. Examples of loss of availability include:

- Power outage or natural disaster;
- Malicious code or denial of service; and
- Equipment failure.

In addition to meeting reporting requirements of existing contracts, an incident of this type should be reported to the RT Information Security Manager within one hour of loss of availability via the e-mail address: **RT.Security@tsa.dhs.gov**.

4. Ongoing Compliance with RT Standards

Under the RT model, SEs contract directly with SPs for services to support RT operations. SEs therefore shall have the primary responsibility of monitoring SP compliance with the RT model, RTIC Technical Interoperability Specification and RT Standards, and for reporting noncompliance to TSA.

TSA shall monitor compliance on an exception basis using the procedures outlined below. These procedures provide guidelines for securing SP information systems and business processes supporting the RT Program.

- **SP self-assessments** shall be performed on an annual basis, not dated 60 days prior to or 60 days following annual attestation. Self-assessments are intended to enable SP management to monitor compliance with RT Standards and self-report compliance deficiencies. SEs shall compile and review SP self-assessments, together with remaining compliance documentation.
- The SP's system(s) shall be subject to **IV&V** reviews conducted by a qualified third party. The third party shall be a qualified Independent Public Accounting (IPA) firm. Reviews shall be conducted in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) No. 10, and TSA guidelines contained in Appendix C. SPs shall obtain an attestation report and TSA's initial approval to provide RT services before commencing operations or the collection of participant enrollment data for transmission to TSA for a security threat assessment.
- The SP's enrollment and verification systems shall be subject to RTIC Technical Interoperability Specification conformance testing by the RT Conformance Lab. Conformance testing is one of the final stages in the process of introducing a new SP into the interoperable RT Program. The purpose of conformance testing is to provide official certification of an SP's technical and procedural ability to comply with all operational and policy requirements outlined in the RTIC Technical Interoperability Specification. SPs must contact TSA to schedule conformance testing. Approval from the RT Conformance Lab is required prior to commencing operations and must occur when any changes are made to SP systems.
- Once the SP starts RT operations, the IV&V reviews shall be conducted periodically, but not less than annually, with the first IV&V review conducted within the first 180 days of operations. The SE is responsible for providing TSA with the IV&V attestation report of its SP. Copies of the IV&V attestation reports shall be provided to TSA with the submission of the attestation report by the IV&V provider to the SE.

All information systems operated by an SP that either directly or indirectly support RT shall be included within the scope of these compliance procedures. Each separate system that composes the SP's RT IT program shall be documented with an SSP (see Section 2.2) as well as a self-assessment. A single IV&V report may be filed, but it must address each system that either directly or indirectly supports RT.

4.1 SP Self-Assessment

Following the completion of the SSP (as described in Section 2.2), SPs shall conduct self-assessments of compliance with RT Standards using the TSA RT SP Self-Assessment Questionnaire contained in Appendix B. One questionnaire is to be completed for each system; there is a 1:1 correspondence between the number of separate systems, the number of SSPs and the number of self-assessments.

Security and control of information system assets and participant data are a fundamental management responsibility. Each SP must implement and maintain adequate security and other internal controls for each system used to support the RT Program directly or indirectly. Security and control are needed to secure participant data and other RT information assets. SP security and control programs must:

- Ensure that systems and applications operate effectively and provide appropriate levels of confidentiality, integrity and availability; and
- Protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access or modification.

4.1.1 Timing

SPs shall perform an initial self-assessment for each subject system and obtain TSA's approval to provide RT services before commencing operations or the collection of participant enrollment data. After TSA's approval to provide RT services is granted, SPs shall conduct self-assessments at least once per calendar year and submit them for review to the SE and to the SP's internal management. Additionally, each SP will maintain the results of the four previous self-assessments as part of their SSPs and for review as a component of the IV&V process.

4.1.2 Self-Assessment Questionnaire

An SP Self-Assessment Questionnaire is provided in Appendix B. This questionnaire contains two sections: Part 1 is the basic system identification and the SP Assertion; part 2 contains the Information Security Program Questions (Control Objectives 1 through 17), the Enrollment/Verification Process Control Questions (Control Objectives 18 and 19) and the Privacy Questions (Control Objective 20).

Part 2 is organized as follows:

There are 20 control objectives, which are numbered 1 through 20, and each has an introductory paragraph that explains the objective concept.

A table then follows each introductory paragraph, with each row containing either no index number, a two-part index number or a three-part index number. For an example, refer to table 4-1, Example of Self-Assessment.

Table 4-1. Example of Self-Assessment

Specific Control Objectives and Techniques	800-53	L.1 Policy	L.2 Procedure	L.3 Implemented	L.4 Tested	L.5 Integrated
Logical Access Controls	AC-1					
16.1. Critical Element: Do the logical access controls restrict users to authorized transactions and functions?						
16.1.1 Can the security controls detect unauthorized access attempts?	AC-3					
16.1.2 Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion?	AC-3 AC-5 AC-6					

The first row, Logical Access Controls, has no index number. The only result that may be recorded is "L.1 Policy" (checking the box) or the lack of a policy (not checking the box). For control objectives with an entry in the 800-53 column (Control Objectives 1 through 17), the SP should review the cited control number (found in Appendix C) and determine whether the system is, or is not, in compliance with the requirement for a policy. If that control objective does not have a policy, the rest of the entries for that objective may be left blank; lack of a policy obviates the relevance of any procedures or their implementation for the entirety of that control objective.

The two-level index numbers are critical elements and are marked as such. These are summary items that reflect the high watermark of every three-level index element (security control) underneath them. They are completed after the results for all of the three-level index elements have been collected.

The three-level index numbers are security controls. For Control Objectives 1 through 17, these index numbers cite one or more 800-53 control numbers, which can be found in Appendix C of the standards. For each of these, the SP should refer to the cited control in Appendix C before recording its self-assessment data in the row for that control objective.

Each control objective is recorded with only one level of compliance as shown in table 4-1; either a policy exists or it does not. Critical elements and security controls use levels two through five of table 4-2, Levels of Security Effectiveness.

Table 4-2. Levels of Security Effectiveness

Level	Description
Level 1	Documented Policy
Level 2	Documented Procedures
Level 3	Implemented Procedures and Controls
Level 4	Tested and Reviewed Procedures and Controls
Level 5	Fully Integrated Procedures and Controls

The definitions for each of the five levels are found in Appendix C, Federal IT Security Assessment Framework to NIST Special Publication 800-26, available at **http://csrc.nist.gov**. SPs should ensure that they review the framework and fully understand the requirements of self-reporting any security control or critical element at a given level of implementation and compliance.

Each level is cumulative. For example, unless Level 1 has been met (policy) at the control objective level, none of the rest of the elements within the objective should be documented.

Level 2 can be assigned to a security control if the control objective has attained Level 1, the 800-53 control solution is recorded as mandated by the NIST SP 800-26 Appendix C and the procedure has been documented in the SSP. Note that some security controls have multiple citations to 800-53 controls and that all of them must obtain a level before the security control as a whole can be reported at that level.

Level 3 can be assigned if Level 2 has been assigned, the security control solution (the procedure) is implemented as mandated by the NIST SP 800-26 Appendix C, the procedure has been implemented in accordance with the SSP and the procedure fully complies with the requirement of the 800-53 control.

Level 4 can be assigned if Level 3 has been assigned, the security control solution is tested as mandated by the NIST SP 800-26 Appendix C, the recommended audit technique from Appendix C of the RT Standards has been performed, the results showed compliance with the security control requirement and the results have been documented.

Level 5 can be assigned if Level 4 has been assigned, the security control is integrated into a total information security lifecycle that collects and utilizes metrics, the integration has been done and is sustained as mandated by the NIST SP 800-26 Appendix C and an explanation of how this has been done is supplied in the notes section of that control objective.

Once each security control within a critical element is documented, the cumulative result for that critical item can be recorded. The critical element is to be marked at the lowest level found for any security control within that element.

For Control Objectives 18 through 20, Level 1 is attained automatically because the RT Standards provide the policy that requires these objectives. Each security control should be assessed again, but no 800-53 guidance is available for these; they should be based strictly on the material supplied in Appendix C of the RT Standards. Again, the critical element as a whole attains the lowest level of compliance of all of the security controls within it.

Comments must be included for any risk-based decision entries. For security controls that cannot be met, a rationale as to the reason why the risk should be assumed, along with an analysis that must be cited in the comments field, and sufficient explanation must be provided in the notes section for that control objective. SPs that use risk-based decisions will be subjected to scrutiny regarding the justification, rationale, and residual risk.

Comments also may be supplied if explanatory information would assist the EP, TSA or IPA firm in evaluating the self-assessment.

Critical elements and security controls rows have an initials box at the end of each row. The individual who has made the "level determination" for that item must initial in that box. These individuals are expected to have cognizant insight and understanding of the self-assessment results that they are documenting, and they may be required (for example, by the IPA firm) to explain their understanding of, and rationale for, the items that they have initialed.

4.1.3 Reporting Instructions

Each SP is expected to complete Part 1 and Part 2 of the initial self-assessment questionnaire for each system in the SP's RT IT program. The self-assessment report shall include the completed questionnaire, along with the SP management assertion statement indicating compliance with RT Standards and required controls as well as any exceptions or risks associated with the SP's security program.

4.2 Independent Verification and Validation

SPs shall obtain annual attestation reports of RT Standards compliance from an IPA firm. The attestation reports shall be conducted in accordance with AICPA SSAE No. 10 and TSA guidelines. The recommended procedures to be performed as part of this attestation are included in Appendix C. Sample attestation report formats are included in Appendix D.

4.2.1 IPA Firm Selection

SPs are required to contract with a qualified IPA firm to perform an attestation of the SP's compliance with RT Standards and required controls. IPA firm selection shall be subject to relevant AICPA guidance regarding independence. Further consideration shall be given to the IPA firm's capabilities to assess information system security and process controls. TSA reserves the right to reject an IPA firm's attestation if, in TSA's judgment, the firm is not sufficiently qualified to perform these services.

4.2.2 Timing

SPs shall obtain an attestation report and TSA's initial approval to provide RT services before commencing operations or the collection of participant enrollment data for transmission to TSA for a security threat assessment.

Following the granting of TSA's approval to provide RT services, SPs shall obtain an attestation report at least annually for the duration of the SP's participation in the RT Program. The first such attestation is due to TSA on or before the sixth month following initial approval to provide RT services. Subsequent attestations are due to TSA every 12 months thereafter.

4.2.3 Compliance Assessment Procedures

The procedures for assessing compliance with RT Standards are included in Appendix C. IPA firms shall follow the procedures outlined in this document in conducting their attestation.

4.2.4 Attestation Report Format

AICPA SSAE No. 10 provides the required reporting guidelines for the attestation report. Sample report formats are included in Appendix D. The IPA firm shall follow the guidelines included in SSAE No. 10 with regard to the reporting of scope limitation, material weaknesses or other necessary disclosures.

The objective of the IPA attestation is the expression of an opinion on whether the SP's management assertion is stated fairly in all material respects. The IPA firm's ability to express an opinion and the wording of the IPA firm's opinion will depend on the facts and circumstances at the date of the IPA firm's attestation report. If for any reason the IPA firm is unable to complete the examination, has not formed an opinion or is unable to form an opinion, the IPA firm may decline to express an opinion or decline to issue a report as a result of the engagement.

4.2.5 Reporting Instructions

IPA firms shall send a copy of their signed attestation reports directly to the SE and to TSA at:

Registered Traveler Program
Office of Transportation Threat Assessment and Credentialing (TTAC)
TSA-19, Transportation Security Administration
601 South 12th Street
Arlington, VA 22202-4220

Alternatively, IPA firms may submit password-protected attestation reports electronically to:

RT.Standards@tsa.dhs.gov.

The subject line of the e-mail shall include the SE names and "Attestation Report."

All e-mails submitted must be smaller than 5 megabytes (MB). Divide submissions larger than 5 MB into multiple e-mails and include in the subject line: SE names, the phrase "Attestation Report," and # of # e-mails. TSA will not accept any electronic submission determined to contain a virus.

4.3 Review of Compliance Documentation

Under the RT model, SEs contract directly with SPs for services to support RT operations. Because of this contractual relationship, SEs shall have the primary responsibility of monitoring SP compliance with the RT model, RTIC Technical Interoperability Specification and RT Standards.

TSA will review the attestation report and any accompanying documentation to determine whether an SE or SP complies with RT Standards. TSA may identify issues or risks either included in compliance documentation or in information otherwise available to TSA that indicate noncompliance with RT Standards. SEs that do not comply with RT Standards have no more than 72 hours from the date of notification by TSA to remedy compliance deficiencies. Severe deficiencies may require remediation more promptly than 72 hours.

With regard to identified deficiencies, TSA reserves the right to:

- Require SEs to remediate severe deficiencies sooner than 72 hours if such deficiencies represent an immediate risk to the security of participant data or other RT Program operations;
- Immediately suspend or revoke its approval to provide RT services and/or disconnect RT systems from the CIMS if significant areas of noncompliance are not remedied as required by TSA; and
- Independently verify that corrective actions to address compliance deficiencies are operating effectively to mitigate the risk associated with such deficiencies.

Each SE will include a provision in its contract with its SPs authorizing TSA oversight. Oversight may include announced, unannounced and/or unscheduled inspections of the SP. Failure of an SP to comply with RT Standards or to cooperate with TSA or its contractors will be considered by TSA in decisions regarding the ongoing participation of an SP in the RT Program. In addition, each SE will require each of its SPs to obtain express written authorization allowing TSA to audit or inspect the security controls over the SP's RT Program, including performing vulnerability assessments and conformance testing.

4.4 Baseline Reporting

Baseline reporting will provide the RT PMO with a quantitative report outlining the operational aspects of routine SP activities. These reports are divided into three categories: enrollment operations, verification station operations and equipment operations.

4.4.1 Enrollment Operations

Capturing and measuring enrollment performance will enable the RT PMO to assess program effectiveness. Specifically, the SP shall report the number of failures to enroll due to inability to meet program requirements. Causes of a failure to enroll may include a lack of verifiable paperwork, insufficient biometrics, or failure to meet any other program requirements.

4.4.2 Verification Station Operations

Measuring verification station operations enables the RT PMO to measure program effectiveness, overall use and impacts to airport operations and security. Specifically, the SP shall report:

- Ratio of verifications (fingerprints to iris scans); and
- Ratio of secondary biometrics (secondary biometric to primary biometric).

4.4.3 Equipment Operations

Measuring equipment operational performance provides the RT PMO with insight into the availability of operations and the effectiveness of the RT Standards. Specifically, the SP shall report:

- Percentage of total equipment availability during operational hours; and
- Causes of loss of availability (e.g., demand maintenance or equipment failure).

4.4.4 Reporting Frequency and Format

SPs shall report these metrics on a monthly basis via e-mail on the last business day of the month to the RT Security Officer (**RT.Security@tsa.dhs.gov**) using the format outlined in table 4-3, Monthly RT Baseline Metrics Report.

Table 4-3. Monthly RT Baseline Metrics Report

Monthly RT Baseline Metrics Report			
SP Name:		**Date:**	
Enrollment Operations	Number of failures to enroll due to inability to meet program requirements		
Verification Station Operations	Ratio of verifications (fingerprints to iris scans)		
	Ratio of times a secondary biometric must be used		
Equipment Operations	Percent of total equipment availability during operations		
	Causes of loss of availability		

Homeland Security

RT Registered Traveler™